Prvočísla

Michal Bulant

Masarykova univerzita
Přírodovědecká fakulta

26. 2. 2010

Obsah přednášky

Plán přednášky

Prvočíslo

Definice

Přirozené číslo, které má právě 2 kladné dělitele, se nazývá **prvočíslo**.

Prvočíslo

Definice

Přirozené číslo, které má právě 2 kladné dělitele, se nazývá **prvočíslo**.

Definice (alternativní)

Přirozené číslo n je prvočíslo, právě když pro libovolná $a, b \in \mathbb{Z}$ platí

$$p \mid ab \implies p \mid a \text{ nebo } p \mid b.$$

Prvočíslo

Definice

Přirozené číslo, které má právě 2 kladné dělitele, se nazývá **prvočíslo**.

Definice (alternativní)

Přirozené číslo n je prvočíslo, právě když pro libovolná $a, b \in \mathbb{Z}$ platí

$$p \mid ab \implies p \mid a \text{ nebo } p \mid b.$$

Je vidět, že obě definice popisují totéž?

Prvočíslo

Definice

Přirozené číslo, které má právě 2 kladné dělitele, se nazývá **prvočíslo**.

Definice (alternativní)

Přirozené číslo n je prvočíslo, právě když pro libovolná $a, b \in \mathbb{Z}$ platí

$$p \mid ab \implies p \mid a \text{ nebo } p \mid b.$$

Je vidět, že obě definice popisují totéž?

Věta (Základní věta aritmetiky)

Každé přirozené číslo se dá jednoznačně (až na pořadí) zapsat jako součin prvočísel.

Prvočísel je ∞ – I. Eukleides apod.

Existuje spousta (ale jen konečně mnoho :) důkazů. Obvykle se postupuje sporem, kdy se všechna předpokládaná prvočísla označí jako $p_1 < p_2 < ldots < p_k$:

Eukleides $p_1 p_2 \cdots p_k + 1$

Kummer $N = p_1 p_2 \cdots p_k$, pak $N - 1$ je násobkem prvočísla p_i, proto i $N - (N - 1) = 1$.

Stieltjes Rozložme $N = p_1 p_2 \cdots p_k$ na součin mn (jakkoliv). Každé prvočíslo dělí právě jedno z čísel m, n, proto $m + n$ není žádným z nich dělitelné (a to je samozřejmě spor).

Prvočísel je ∞ – II. posloupnosti

Je snadno vidět, že pokud se podaří sestavit **nekonečnou** posloupnost **po dvou nesoudělných** přirozených čísel (větších než 1), existuje nutně nekonečně mnoho prvočísel.

Prvočísel je ∞ – II. posloupnosti

Je snadno vidět, že pokud se podaří sestavit **nekonečnou** posloupnost **po dvou nesoudělných** přirozených čísel (větších než 1), existuje nutně nekonečně mnoho prvočísel.

Věta (Goldbach, 1730)

Fermatova čísla $F_n = 2^{2^n} + 1$ jsou po dvou nesoudělná.

Prvočísel je ∞ – II. posloupnosti

Je snadno vidět, že pokud se podaří sestavit **nekonečnou** posloupnost **po dvou nesoudělných** přirozených čísel (větších než 1), existuje nutně nekonečně mnoho prvočísel.

Věta (Goldbach, 1730)

Fermatova čísla $F_n = 2^{2^n} + 1$ jsou po dvou nesoudělná.

Důkaz.

Snadno se indukcí dokáže, že $F_0 F_1 \cdots F_m = F_{m+1} - 2$, odkud už snadno vyplyne, že F_n jsou po dvou nesoudělná. □

S využitím vlastností největšího společného dělitele a toho, že je možné jej vypočítat pomocí tzv. Eukleidova algoritmu plyne následující:

Lemma

Pro $1 \leq i < j \leq n$ *platí* $(i \cdot (n!) + 1, j \cdot (n!) + 1) = 1$.

S využitím vlastností největšího společného dělitele a toho, že je možné jej vypočítat pomocí tzv. Eukleidova algoritmu plyne následující:

Lemma

Pro $1 \leq i < j \leq n$ *platí* $(i \cdot (n!) + 1, j \cdot (n!) + 1) = 1$.

Kdyby existovalo pouze k prvočísel, tak z předchozího lemmatu s volbou $n = k + 1$ dostáváme posloupnost n po dvou nesoudělných čísel, což je opět spor.

Prvočísel je ∞ – III. nekonečné řady (Euler)

Eulerův důkaz není úplně přímočarý, ale poskytuje silnější tvrzení než pouze nekonečnost počtu prvočísel.

Prvočísel je ∞ – III. nekonečné řady (Euler)

Eulerův důkaz není úplně přímočarý, ale poskytuje silnější tvrzení než pouze nekonečnost počtu prvočísel.
Sestavíme pro každé prvočíslo p nekonečnou geometrickou řadu $\sum_{l=0}^{\infty} \frac{1}{p^l}$, jejíž součet je $\frac{1}{1-1/p}$.

Prvočísel je ∞ – III. nekonečné řady (Euler)

Eulerův důkaz není úplně přímočarý, ale poskytuje silnější tvrzení než pouze nekonečnost počtu prvočísel.
Sestavíme pro každé prvočíslo p nekonečnou geometrickou řadu $\sum_{l=0}^{\infty} \frac{1}{p^l}$, jejíž součet je $\frac{1}{1-1/p}$. Jsou-li opět $p_1, \ldots, p_k$ všechna prvočísla, pak vynásobením příslušných k geometrických řad dostaneme

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{i=1}^{k} \frac{1}{1-1/p_i}.$$

Prvočísel je ∞ – III. nekonečné řady (Euler)

Eulerův důkaz není úplně přímočarý, ale poskytuje silnější tvrzení než pouze nekonečnost počtu prvočísel.
Sestavíme pro každé prvočíslo p nekonečnou geometrickou řadu $\sum_{l=0}^{\infty} \frac{1}{p^l}$, jejíž součet je $\frac{1}{1-1/p}$. Jsou-li opět $p_1, \ldots, p_k$ všechna prvočísla, pak vynásobením příslušných k geometrických řad dostaneme

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{i=1}^{k} \frac{1}{1-1/p_i}.$$

Přitom se ale snadno dokáže, že řada $\sum_{n=1}^{\infty} \frac{1}{n}$ diverguje (tj. roste nade všechny meze), zatímco výraz na pravé straně je zřejmě konečný.

Prvočísel je ∞ – III. nekonečné řady (Euler)

Eulerův důkaz není úplně přímočarý, ale poskytuje silnější tvrzení než pouze nekonečnost počtu prvočísel.
Sestavíme pro každé prvočíslo p nekonečnou geometrickou řadu $\sum_{l=0}^{\infty} \frac{1}{p^l}$, jejíž součet je $\frac{1}{1-1/p}$. Jsou-li opět $p_1, \ldots, p_k$ všechna prvočísla, pak vynásobením příslušných k geometrických řad dostaneme

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{i=1}^{k} \frac{1}{1-1/p_i}.$$

Přitom se ale snadno dokáže, že řada $\sum_{n=1}^{\infty} \frac{1}{n}$ diverguje (tj. roste nade všechny meze), zatímco výraz na pravé straně je zřejmě konečný.

Poznámka

Obdobným způsobem se dá dokonce dokázat, že řada $\sum_{p \in P} \frac{1}{p}$ diverguje.

Plán přednášky

1. Co je to prvočíslo a kolik jich je?

2. Jak poznat prvočísla?
   - Teoretické základy
   - Klasické testy s využitím kongruencí
   - Mersenneho prvočísla

Eratosthenovo síto

Známá metoda, která poskytuje postup, jak nalézt dokonce všechna prvočísla až do jisté hranice.
Její jediný, zato však zásadní problém, je časová náročnost – pro zjištění prvočísel až do velikosti N potřebujeme znát prvočísla až do velikosti $\sqrt{N}$, což je obvykle příliš mnoho.

Některé důležité věty

Věta (Fermatova)

Je-li a nedělitelné prvočíslem p, pak $p \mid a^{p-1} - 1$, tj.

$$a^{p-1} \equiv 1 \pmod{p}.$$

Některé důležité věty

Věta (Fermatova)

Je-li a nedělitelné prvočíslem p, pak $p \mid a^{p-1} - 1$, tj.

$$a^{p-1} \equiv 1 \pmod{p}.$$

Důkaz.

Důkaz viz [Kondr] (nebo [Euler]). □

Eulerova funkce

Základní vlastnosti:

- $\varphi(p) = p - 1$
- $\varphi(p^k) = (p-1)p^{k-1}$
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ pro $(a, b) = 1$.

Některé důležité věty II.

Věta (Eulerova)

Je-li $a \in \mathbb{Z}, m \in \mathbb{N}$ *a* $(a, m) = 1$, *pak*

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

kde $\varphi(m)$ *označuje tzv. Eulerovu funkci, udávající počet přirozených čísel nepřevyšujících* m, *která jsou s* m *nesoudělná.*

Některé důležité věty II.

Věta (Eulerova)

Je-li $a \in \mathbb{Z}, m \in \mathbb{N}$ *a* $(a, m) = 1$, *pak*

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

kde $\varphi(m)$ *označuje tzv. Eulerovu funkci, udávající počet přirozených čísel nepřevyšujících* m, *která jsou s* m *nesoudělná.*

Věta (Wilsonova)

Přirozené číslo n *je prvočíslo, právě když*

$$(n-1)! \equiv -1 \pmod{n}.$$

Řád čísla modulo, primitivní kořen

Definice

Řádem čísla a modulo m, kde $(a, m) = 1$, nazveme nejmenší přirozené číslo r takové, že $a^r \equiv 1 \pmod{m}$.

Fakt

- $r \mid \varphi(m)$;
- modulo prvočíslo p existuje právě $\varphi(p-1)$ čísel řádu $\varphi(p) = p - 1$ modulo p (menších než p), jde o takzvané primitivní kořeny.

Kvadratické (ne)zbytky

Definice

Buď p prvočíslo. Číslo a splňující $(a, p) = 1$ nazveme kvadratickým zbytkem modulo p, jestliže existuje x takové, že $x^2 \equiv a \pmod{p}$, v opačném případě jde o kvadratický nezbytek. Píšeme $(a/p) = 1$, resp. $(a/p) = -1$ (Legendreův symbol). Dále pro $p \mid a$ píšeme $(a/p) = 0$.

Kvadratické (ne)zbytky

Definice

Buď p prvočíslo. Číslo a splňující $(a, p) = 1$ nazveme kvadratickým zbytkem modulo p, jestliže existuje x takové, že $x^2 \equiv a \pmod{p}$, v opačném případě jde o kvadratický nezbytek. Píšeme $(a/p) = 1$, resp. $(a/p) = -1$ (Legendreův symbol). Dále pro $p \mid a$ píšeme $(a/p) = 0$.

Fakt

- $(a/p) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
- pro $a \equiv b \pmod{p}$ platí $(a/p) = (b/p)$.
- $(a \cdot b/p) = (a/p) \cdot (b/p)$.
- $(-1/p) = (-1)^{\frac{p-1}{2}}$,
  $(2/p) = (-1)^{\frac{p^2-1}{8}}, (p/q) = (q/p) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Klasické testy s využitím kongruencí

Wilsonova věta dává sice nutnou i postačující podmínku prvočíselnosti, bohužel nikdo na světě dosud neumít *rychle* vypočítat faktoriál modulo velké číslo. Proto využijeme ostatní věty, které sice dávají pouze nutnou podmínku prvočíselnosti (*je-li p prvočíslo, pak ...*).

Klasické testy s využitím kongruencí

Wilsonova věta dává sice nutnou i postačující podmínku prvočíselnosti, bohužel nikdo na světě dosud neumít *rychle* vypočítat faktoriál modulo velké číslo. Proto využijeme ostatní věty, které sice dávají pouze nutnou podmínku prvočíselnosti (*je-li p prvočíslo, pak ...*).
Takovým testem je např. klasický Fermatův test plynoucí ze stejnojmenné věty.

Fermatův test

Existuje-li pro dané N nějaké a takové, že $a^{N-1} \not\equiv 1 \pmod{N}$, pak N není prvočíslo.

Fermatův test není ideální

Bohužel nemusí být pro dané složené N snadné najít a takové, že Fermatův test odhalí složenost N, pro některá výjimečná N dokonce jediná taková a jsou soudělná s N, jejich nalezení je tedy ekvivalentní s rozkladem N na prvočísla.

Fermatův test není ideální

Bohužel nemusí být pro dané složené N snadné najít a takové, že Fermatův test odhalí složenost N, pro některá výjimečná N dokonce jediná taková a jsou soudělná s N, jejich nalezení je tedy ekvivalentní s rozkladem N na prvočísla.
Skutečně existují taková nehezká (nebo extrémně hezká?) složená čísla N, která splňují, že pro libovolné a nesoudělné s N platí $a^{N-1} \equiv 1 \pmod{N}$. Taková čísla se nazývají Carmichaelova, nejmenší z nich je $561 = 3 \cdot 11 \cdot 17$ a teprve v roce 1992 se podařilo dokázat, že jich je dokonce nekonečně mnoho.

Fermatův test není ideální

Bohužel nemusí být pro dané složené N snadné najít a takové, že Fermatův test odhalí složenost N, pro některá výjimečná N dokonce jediná taková a jsou soudělná s N, jejich nalezení je tedy ekvivalentní s rozkladem N na prvočísla.
Skutečně existují taková nehezká (nebo extrémně hezká?) složená čísla N, která splňují, že pro libovolné a nesoudělné s N platí $a^{N-1} \equiv 1 \pmod{N}$. Taková čísla se nazývají Carmichaelova, nejmenší z nich je $561 = 3 \cdot 11 \cdot 17$ a teprve v roce 1992 se podařilo dokázat, že jich je dokonce nekonečně mnoho.
Fermatův test lze zlepšit s využitím kvadratických zbytků na Eulerův test $a^{\frac{N-1}{2}} \equiv (a/N) \pmod{N}$, ale výše zmíněný problém se zcela neodstraní ani tímto vylepšením.

Fermatův test není ideální

Bohužel nemusí být pro dané složené N snadné najít a takové, že Fermatův test odhalí složenost N, pro některá výjimečná N dokonce jediná taková a jsou soudělná s N, jejich nalezení je tedy ekvivalentní s rozkladem N na prvočísla.

Skutečně existují taková nehezká (nebo extrémně hezká?) složená čísla N, která splňují, že pro libovolné a nesoudělné s N platí $a^{N-1} \equiv 1 \pmod{N}$. Taková čísla se nazývají Carmichaelova, nejmenší z nich je $561 = 3 \cdot 11 \cdot 17$ a teprve v roce 1992 se podařilo dokázat, že jich je dokonce nekonečně mnoho.

Fermatův test lze zlepšit s využitím kvadratických zbytků na Eulerův test $a^{\frac{N-1}{2}} \equiv (a/N) \pmod{N}$, ale výše zmíněný problém se zcela neodstraní ani tímto vylepšením.

V praxi se často používají další vylepšení, zejména tzv. Rabin-Millerův test.

Test prvočíselnosti

Ukázali jsme si, jak je možné odhalit složená čísla. Co ale s těmi, která tento test za složená neoznačí? Jsou to prvočísla nebo čísla složená. K ověření toho, slouží (časově daleko náročnější) testy na prvočíselnost.

Lucas-Lehmer

Pokud pro libovolný prvočíselný dělitel q čísla $N-1$ existuje a tak, že $a^{N-1} \equiv 1 \pmod{N}$, $a^{\frac{N-1}{q}} \not\equiv 1 \pmod{N}$, pak je N prvočíslo.

Test prvočíselnosti

Ukázali jsme si, jak je možné odhalit složená čísla. Co ale s těmi, která tento test za složená neoznačí? Jsou to prvočísla nebo čísla složená. K ověření toho, slouží (časově daleko náročnější) testy na prvočíselnost.

Lucas-Lehmer

Pokud pro libovolný prvočíselný dělitel q čísla $N-1$ existuje a tak, že $a^{N-1} \equiv 1 \pmod{N}$, $a^{\frac{N-1}{q}} \not\equiv 1 \pmod{N}$, pak je N prvočíslo.

Důkaz.

Stačí dokázat, že $N-1$ dělí $\varphi(N)$. Pokud ne, tak existuje prvočíslo q a $r \in \mathbb{N}$ tak, že q^r dělí $N-1$, ale ne $\varphi(N)$. Řád e prvku a dělí $N-1$ (první podmínka) a nedělí $(N-1)/q$ (druhá podmínka), proto q^r dělí e. Navíc e dělí $\varphi(N)$, tedy i q^r dělí $\varphi(N)$, spor. $\square$

Test prvočíselnosti II.

Předchozí test má tu nevýhodu, že je třeba umět kompletně rozložit $N - 1$ na prvočísla. To je snadné třeba u Fermatových čísel, ale obvykle je to obtížné. Proto je užitečné mít k dispozici variantu tohoto testu, která kompletní faktorizaci nepožaduje – viz např. test Pocklingtona a Lehmera.

Test prvočíselnosti II.

Předchozí test má tu nevýhodu, že je třeba umět kompletně rozložit $N - 1$ na prvočísla. To je snadné třeba u Fermatových čísel, ale obvykle je to obtížné. Proto je užitečné mít k dispozici variantu tohoto testu, která kompletní faktorizaci nepožaduje – viz např. test Pocklingtona a Lehmera.

Poznámka

Veškeré předchozí testy *strčili do kapsy* v roce 2002 indičtí matematici Agrawal, Kayal a Saxena, kteří Fermatův test aplikovali ve složitější algebraické situaci a odvodili z něj test, který je polynomiální časové složitosti (do té doby se vůbec nevědělo, jakou složitost tohoto problému očekávat).

Fermatova prvočísla

Zmínili jsme se už o speciálních číslech tvaru $F_m = 2^{2^m} + 1$. Jinak geniální právník Pierre de Fermat vyslovil domněnku, že všechna tato čísla jsou prvočísly. Protože tato čísla enormně rychle rostou, o F_5 už to nebyl schopen ověřit tehdejšími prostředky. Ukážeme Eulerův geniální důkaz, že $641 \mid F_5$; do dnešních dnů nebylo nalezeno žádné další Fermatovo prvočíslo, navíc i jejich faktorizace nejde nijak závratným tempem – největší úplně rozložené Fermatovo číslo je F_{11}, největší Fermatovo číslo, o němž je známo, že je složené je F_{23471} s dělitelem $5 \cdot 2^{23473} + 1$.

Poznámka

Do dnešních dnů se neví odpověď ani na jednu z následujících zásadních otázek:

- Existuje ∞ Fermatových prvočísel?
- Existuje ∞ Fermatových složených čísel?

F_5 je složené

Věta

Každý prvočíselný faktor $F_n (n \geq 2)$ je tvaru $k \times 2^{n+2} + 1$.

F_5 je složené

Věta

Každý prvočíselný faktor $F_n (n \geq 2)$ je tvaru $k \times 2^{n+2} + 1$.

Důkaz.

Buď p prvočíselný faktor F_n. Řád 2 modulo p je tedy právě 2^{n+1}, odkud $2^{n+1} \mid p-1$, speciálně $8 \mid p-1$. Odtud $2^{\frac{p-1}{2}} \equiv (2/p) = 1 \pmod{p}$, a tedy $2^{n+1} \mid \frac{p-1}{2}$. □

F_5 je složené

Věta

Každý prvočíselný faktor $F_n (n \geq 2)$ je tvaru $k \times 2^{n+2} + 1$.

Důkaz.

Buď p prvočíselný faktor F_n. Řád 2 modulo p je tedy právě 2^{n+1}, odkud $2^{n+1} \mid p-1$, speciálně $8 \mid p-1$. Odtud $2^{\frac{p-1}{2}} \equiv (2/p) = 1 \pmod{p}$, a tedy $2^{n+1} \mid \frac{p-1}{2}$. □

$641 \mid F_5$

$$F_5 = 33294320 \times (1 \cdot 2^7 + 1) + 17$$
$$F_5 = 16711935 \times (2 \cdot 2^7 + 1) + 2$$
$$F_5 = 11155759 \times (3 \cdot 2^7 + 1) + 82$$
$$F_5 = 8372255 \times (4 \cdot 2^7 + 1) + 482$$
$$F_5 = 6700417 \times (5 \cdot 2^7 + 1) + 0$$

Pepinův test prvočíselnosti F_m

Připomeňme, že Lucas-Lehmerův test prvočíselnosti vyžadoval kompletní faktorizaci $N-1$, to je ale u Fermatových číslech samozřejmé. V naší situaci test říká, že pokud existuje a tak, že $a^{F_m-1} \equiv 1 \pmod{F)_m}$ a $a^{\frac{F_m-1}{2}} \not\equiv 1 \pmod{F_m}$, pak je F_m prvočíslo.

Pepinův test prvočíselnosti F_m

Připomeňme, že Lucas-Lehmerův test prvočíselnosti vyžadoval kompletní faktorizaci $N-1$, to je ale u Fermatových číslech samozřejmé. V naší situaci test říká, že pokud existuje a tak, že $a^{F_m-1} \equiv 1 \pmod{F)_m}$ a $a^{\frac{F_m-1}{2}} \not\equiv 1 \pmod{F_m}$, pak je F_m prvočíslo.

Pepinův test

Pro $k, n \geq 2$ je ekvivalentní:

1. F_n je prvočíslo, $(k/F_n) = -1$,
2. $k^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.

Pepinův test prvočíselnosti F_m

Připomeňme, že Lucas-Lehmerův test prvočíselnosti vyžadoval kompletní faktorizaci $N-1$, to je ale u Fermatových číslech samozřejmé. V naší situaci test říká, že pokud existuje a tak, že $a^{F_m-1} \equiv 1 \pmod{F)_m}$ a $a^{\frac{F_m-1}{2}} \not\equiv 1 \pmod{F_m}$, pak je F_m prvočíslo.

Pepinův test

Pro $k, n \geq 2$ je ekvivalentní:

1. F_n je prvočíslo, $(k/F_n) = -1$,
2. $k^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.

Poznámka

Vhodné volby k jsou třeba $3, 5, 10$, protože $(3/F_n) = (5/F_n) = (10/F_n) = -1$.

Konstrukce pravítkem a kružítkem

S Fermatovými čísly souvisí vynikající výsledek C.F.Gausse, který dokázal, že pravidelný n-úhelník je možné sestrojit pravítkem a kružítkem, právě když je $n = 2^k p_1 p_2 \cdots p_h$, kde p_i jsou po dvou různá Fermatova prvočísla.

Mersenneho prvočísla

Podíváme-li se do tabulek největších známých prvočísel, neujde naší pozornosti, že obvykle jsou všechna tvaru $2^m - 1$.
Má-li být číslo tvaru $2^m - 1$ prvočíslem, je snadným cvičením, že i m musí být prvočíslo. Čísla tvaru $M_q = 2^q - 1$, kde q je prvočíslo, se nazývají Mersenneho čísla[1].

[1] Kněz Marin Mersenne byl Fermatovým současníkem a dopisoval si s ním.

Mersenneho prvočísla

Podíváme-li se do tabulek největších známých prvočísel, neujde naší pozornosti, že obvykle jsou všechna tvaru $2^m - 1$.
Má-li být číslo tvaru $2^m - 1$ prvočíslem, je snadným cvičením, že i m musí být prvočíslo. Čísla tvaru $M_q = 2^q - 1$, kde q je prvočíslo, se nazývají Mersenneho čísla[1].

Věta

Je-li q prvočíslo, $q \equiv 3 \pmod 4$, pak $2q+1$ dělí M_q právě když $2q+1$ je prvočíslo.

Příklad

Odtud např. $23 \mid M_{11}, 47 \mid M_{23}, 83 \mid M_{167}$, *atd*.

[1] Kněz Marin Mersenne byl Fermatovým současníkem a dopisoval si s ním.

Důkaz.

Nechť $n = 2q + 1$ je dělitel M_q. Protože $2^2 \not\equiv 1 \pmod{n}, (-2)^q \not\equiv 1 \pmod{n}$, máme $2^{2q} - 1 = (2^q + 1)M_q \equiv 0 \pmod{n}$ a odtud Lucas-Lehmerovým testem vidíme, že n je prvočíslo.

Důkaz.

Nechť $n = 2q + 1$ je dělitel M_q. Protože $2^2 \not\equiv 1 \pmod{n}, (-2)^q \not\equiv 1 \pmod{n}$, máme $2^{2q} - 1 = (2^q + 1)M_q \equiv 0 \pmod{n}$ a odtud Lucas-Lehmerovým testem vidíme, že n je prvočíslo. Nechť obráceně je $p = 2q + 1 \equiv \pmod{8}$ prvočíslo. Protože $(2/p) = 1$, existuje m tak ,že $2 \equiv m^2 \pmod{p}$. Odtud $2^q \equiv 2^{\frac{p-1}{2}} \equiv m^{p-1} \equiv 1 \pmod{p}$, a tedy $p \mid M_q$. □

Důkaz.

Nechť $n = 2q + 1$ je dělitel M_q. Protože $2^2 \not\equiv 1 \pmod{n}, (-2)^q \not\equiv 1 \pmod{n}$, máme $2^{2q} - 1 = (2^q + 1)M_q \equiv 0 \pmod{n}$ a odtud Lucas-Lehmerovým testem vidíme, že n je prvočíslo. Nechť obráceně je $p = 2q + 1 \equiv \pmod{8}$ prvočíslo. Protože $(2/p) = 1$, existuje m tak ,že $2 \equiv m^2 \pmod{p}$. Odtud $2^q \equiv 2^{\frac{p-1}{2}} \equiv m^{p-1} \equiv 1 \pmod{p}$, a tedy $p \mid M_q$. □

Věta

Pokud n dělí M_q, pak $n \equiv \pm 1 \pmod{8}$ a $n \equiv 1 \pmod{q}$.

Důkaz.

Nechť $n = 2q + 1$ je dělitel M_q. Protože $2^2 \not\equiv 1 \pmod{n}, (-2)^q \not\equiv 1 \pmod{n}$, máme $2^{2q} - 1 = (2^q + 1)M_q \equiv 0 \pmod{n}$ a odtud Lucas-Lehmerovým testem vidíme, že n je prvočíslo. Nechť obráceně je $p = 2q + 1 \equiv \pmod{8}$ prvočíslo. Protože $(2/p) = 1$, existuje m tak ,že $2 \equiv m^2 \pmod{p}$. Odtud $2^q \equiv 2^{\frac{p-1}{2}} \equiv m^{p-1} \equiv 1 \pmod{p}$, a tedy $p \mid M_q$. □

Věta

Pokud n dělí M_q, pak $n \equiv \pm 1 \pmod{8}$ a $n \equiv 1 \pmod{q}$.

Důkaz.

Pokud $p \mid M_q = 2^q - 1$, pak $q \mid p - 1$, odkud $2qk = p - 1$ a tedy $(2/p) \equiv 2^{\frac{p-1}{2}} \equiv 2^{qk} \equiv 1 \pmod{p}$, tj. $p \equiv \pm 1 \pmod{8}$. □

Poznámka

Do dnešních dnů se neví odpověď ani na jednu z následujících zásadních otázek:

- Existuje ∞ Mersenneho prvočísel?
- Existuje ∞ Mersenneho složených čísel?

Poznámka

Do dnešních dnů se neví odpověď ani na jednu z následujících zásadních otázek:

- Existuje ∞ Mersenneho prvočísel?
- Existuje ∞ Mersenneho složených čísel?

Dokonalá čísla

Dokonalá čísla jsou čísla se součtem všech dělitelů rovným svému dvojnásobku – např. 6, 28, 496, 8128. Dosud se neví, zda existuje nějaké liché dokonalé číslo, ví se ale, že *každé sudé dokonalé číslo je tvaru* $2^{q-1}(2^q - 1)$, *kde* q *i* $M_q = 2^q - 1$ *jsou prvočísla.*